

INFORMATION PROCESSOR AND METHOD THEREFOR

Patent number: JP2003224561
 Publication date: 2003-08-08
 Inventor: SLICK ROYCE E; ZHANG WILLIAM; PURPURA DON FRANCIS; IWAMOTO NEIL Y; MAZZAGATTE CRAIG
 Applicant: CANON KK
 Classification:
 - international: H04L9/08; G06F3/12; G06F12/14
 - european:
 Application number: JP20020352937 20021204
 Priority number(s): US20010010974 20011205

Also published as:

EP1320009 (A2)
 US2003105963 (A1)

Abstract of JP2003224561

<P>PROBLEM TO BE SOLVED: To provide a constitution capable of securely holding a public key in a computing device which can easily verify the public key every time before use without the need of a certificate or an authentication authority. <P>SOLUTION: A secret key 54 intrinsic to a user is provided to a ciphering algorithm 65 together with a printer public key 25 to generate a ciphered printer public key 67 and it is stored in a registry 41 under the 'user 1' entry 42 of a sub entry 44. Then, before ciphering print data by using the printer public key 25, the already stored version of the printer public key 25 is authenticated. <P>COPYRIGHT: (C)2003,JPO

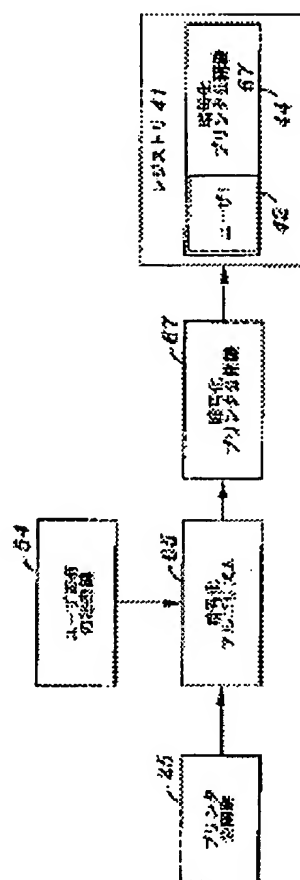


FIG. 4A

Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開2003-224561

(P2003-224561A)

(43) 公開日 平成15年 8 月 8 日 (2003. 8. 8)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
H 0 4 L 9/08		G 0 6 F 3/12	K 5 B 0 1 7
G 0 6 F 3/12		12/14	3 2 0 A 5 B 0 2 1
12/14	3 2 0	H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
			6 0 1 F

審査請求 有 請求項の数32 O L (全 22 頁)

(21) 出願番号 特願2002-352937(P2002-352937)

(22) 出願日 平成14年12月 4 日 (2002. 12. 4)

(31) 優先権主張番号 1 0 / 0 1 0 9 7 4

(32) 優先日 平成13年12月 5 日 (2001. 12. 5)

(33) 優先権主張国 米国 (U S)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子 3 丁目30番 2 号

(72) 発明者 ロイス イー. スリック

アメリカ合衆国 カリフォルニア州

92612, アーバイン, イノベーション ド

ライブ 110 キヤノン デベロップメン

ト アメリカス, インコーポレイテッド

内

(74) 代理人 100076428

弁理士 大塚 康徳 (外 3 名)

最終頁に続く

(54) 【発明の名称】 情報処理装置及びその方法

(57) 【要約】

【課題】 証明書や認証局を必要とすることなく使用前に毎回、公開鍵を容易に検証できる計算装置において公開鍵を機密に保持できる構成が必要となる。

【解決手段】 ユーザ固有の秘密鍵 5 4 をプリンタ公開鍵 2 5 と共に暗号化アルゴリズム 6 5 に提供して暗号化プリンタ公開鍵 6 7 を生成し、これをサブエントリ 4 4 の「ユーザ 1」エントリ 4 2 下にあるレジストリ 4 1 に格納する。そして、プリンタ公開鍵 2 5 を使用してプリントデータを暗号化する前に、プリンタ公開鍵 2 5 の格納済みのバージョンを認証する。

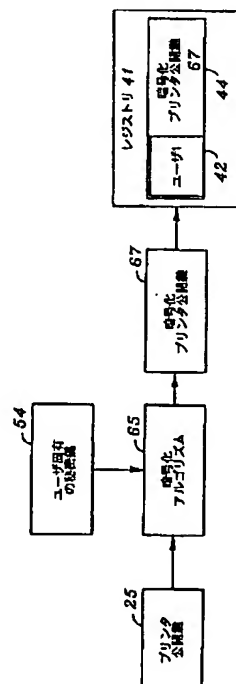


FIG. 4A

【特許請求の範囲】

【請求項1】 ユーザ固有の鍵対を使用し、且つ、データの暗号化のための公開鍵を用いてデータを暗号化する情報処理方法であって、

対象となる装置に対応する対象公開鍵を受信する受信工程と、

機密レジストリからユーザ固有の鍵対を取得する取得工程と、

前記ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して前記対象公開鍵に基づいて対象鍵を検証するためのデータ又はプログラムを作成する鍵暗号化工程と、

前記対象鍵を検証するためのデータ又はプログラムと前記対象公開鍵とを記憶領域に格納する格納工程と、

前記対象鍵を検証するためのデータ又はプログラムと前記対象公開鍵とを記憶領域から抽出する抽出工程と、

前記対象公開鍵の信頼性を検証するために、前記ユーザ固有の鍵対からのユーザ固有の公開鍵を前記対象鍵を検証するためのプログラム又はデータに適用する検証工程と、

前記対象公開鍵の信頼性が検証された場合、データを前記対象公開鍵で暗号化することによって前記対象となる装置に送信するための暗号化データを作成するデータ暗号化工程と、を有することを特徴とする情報処理方法。

【請求項2】 前記計算装置で実行するオペレーティングシステムがサポートする鍵を扱うためのアプリケーション・プログラミング・インタフェースを介して前記ユーザ固有の鍵対を取得することを特徴とする請求項1に記載の情報処理方法。

【請求項3】 前記オペレーティングシステムは、計算装置の複数のユーザのそれぞれに対してユーザ固有の鍵対を機密に保持することを特徴とする請求項2に記載の情報処理方法。

【請求項4】 各ユーザ固有の鍵対に対応するユーザ識別データをオペレーティングシステムに提供することによって前記ユーザ固有の鍵対にアクセスすることができることを特徴とする請求項2又は3に記載の情報処理方法。

【請求項5】 前記鍵暗号化工程で作成された前記対象鍵を検証するためのプログラム又はデータは、前記対象公開鍵の暗号化バージョンであることを特徴とする請求項1乃至4のいずれか1項に記載の情報処理方法。

【請求項6】 前記検証工程は、復号化アルゴリズムを使用して前記ユーザ固有の公開鍵で前記対象鍵を検証するためのプログラム又はデータを復号化することを含むことを特徴とする請求項1乃至5のいずれか1項に記載の情報処理方法。

【請求項7】 前記検証工程は、前記対象公開鍵の信頼性を検証するために、鍵検証アルゴリズムを使用して前記復号化対象鍵を検証するためのプログラム又はデータと前記対象公開鍵とを比較することを更に含むことを特

徴とする請求項6に記載の情報処理方法。

【請求項8】 前記計算装置で実行するオペレーティングシステムがサポートする検証用アプリケーション・プログラミング・インタフェースを介して前記検証工程を行うことを特徴とする請求項7に記載の情報処理方法。

【請求項9】 前記鍵暗号化工程で作成された前記対象鍵を検証するためのプログラム又はデータは、前記対象公開鍵のデジタル署名であることを特徴とする請求項1乃至8のいずれか1項に記載の情報処理方法。

【請求項10】 ハッシングアルゴリズムを前記対象公開鍵に適用して対象鍵ハッシュを取得し、暗号化アルゴリズムを使用して前記対象鍵ハッシュを前記ユーザ固有の秘密鍵で暗号化することによって前記対象公開鍵のデジタル署名を作成することを特徴とする請求項9に記載の情報処理方法。

【請求項11】 ハッシングアルゴリズムを前記対象公開鍵に適用して対象鍵ハッシュを取得し、前記対象鍵ハッシュに対して機密保護アルゴリズムを行うことによって前記対象公開鍵のデジタル署名を作成することを特徴とする請求項9に記載の情報処理方法。

【請求項12】 前記検証工程は、復号化アルゴリズムを使用して前記対象鍵を検証するためのプログラム又はデータを前記ユーザ固有の公開鍵で復号化し、復号化対象鍵ハッシュを取得することを含むことを特徴とする請求項11に記載の情報処理方法。

【請求項13】 前記検証工程は、前記対象公開鍵の信頼性を検証するために、ハッシングアルゴリズムを前記対象公開鍵に再度適用して新たな対象鍵ハッシュを取得し、ハッシュ検証アルゴリズムを使用して前記復号化対象鍵ハッシュと前記新たな対象鍵ハッシュとを比較することを更に含むことを特徴とする請求項12に記載の情報処理方法。

【請求項14】 前記計算装置で実行するオペレーティングシステムがサポートする検証用アプリケーション・プログラミング・インタフェースによって前記検証工程を行うことを特徴とする請求項13に記載の情報処理方法。

【請求項15】 前記抽出工程は、前記受信した対象公開鍵の信頼性を検証するために、ハッシングアルゴリズムを前記受信した対象公開鍵に適用して受信した対象鍵ハッシュを取得し、ハッシュ検証アルゴリズムを使用して前記受信した対象鍵ハッシュとテスト用の対象鍵ハッシュとを比較することを含むことを特徴とする請求項1乃至14のいずれか1項に記載の情報処理方法。

【請求項16】 前記テスト用の対象鍵ハッシュはユーザによって入力されることを特徴とする請求項15に記載の情報処理方法。

【請求項17】 前記対象となる装置は画像形成装置であり、前記テスト用の対象鍵ハッシュを前記画像形成装置によって印刷されたテストページから取得することを

特徴とする請求項16に記載の情報処理方法。

【請求項18】 前記対象となる装置は画像形成装置であり、前記対象公開鍵は画像形成装置公開鍵であることを特徴とする請求項1乃至17のいずれか1項に記載の情報処理方法。

【請求項19】 前記受信工程において、前記画像形成装置に送られた鍵要求に応じて前記画像形成装置公開鍵を受信することを特徴とする請求項18に記載の情報処理方法。

【請求項20】 前記情報処理方法は、前記計算装置で実行するプリンタドライバによって行われることを特徴とする請求項18に記載の情報処理方法。

【請求項21】 ユーザ固有の鍵対を使用し且つ、プリントデータの暗号化のためのプリンタ公開鍵を前記計算装置に機密に格納する情報処理方法において、プリンタに対応するプリンタ公開鍵を受信する受信工程と、

対応するユーザ識別に応じて機密レジストリからユーザ固有の鍵対を取得する取得工程と、ハッシングアルゴリズムを前記プリンタ公開鍵に適用して第1のプリンタ鍵ハッシュを作成する第1のハッシング工程と、

暗号化アルゴリズムを適用して前記ユーザ固有の鍵対からのユーザ固有の秘密鍵で前記第1のプリンタ鍵ハッシュを暗号化することによってプリンタ鍵署名を作成する暗号化工程と、

前記プリンタ鍵署名と前記プリンタ公開鍵とを記憶領域に格納する格納工程と、

前記プリンタ鍵署名と前記プリンタ公開鍵とを記憶領域から抽出する抽出工程と、

前記ハッシングアルゴリズムを前記抽出したプリンタ公開鍵に適用して第2のプリンタ鍵ハッシュを作成する第2のハッシング工程と、

復号化アルゴリズムを適用して前記ユーザ固有の鍵対からのユーザ固有の公開鍵で前記プリンタ鍵署名を復号化することによって前記第1のプリンタ鍵ハッシュを抽出する復号化工程と、

前記抽出したプリンタ公開鍵の信頼性を検証するために、検証アルゴリズムを適用して前記第1のプリンタ鍵ハッシュと前記第2のプリンタ鍵ハッシュとを比較する検証工程と、

前記抽出したプリンタ公開鍵の信頼性が検証された場合、前記抽出したプリンタ公開鍵を使用して暗号化アルゴリズムをプリントデータに適用することによって前記プリンタに送信するための暗号化プリントデータを作成するプリントデータ暗号化工程と、を有することを特徴とする情報処理方法。

【請求項22】 計算装置で受信した画像形成装置の公開鍵の信頼性を検証する情報処理方法において、画像形成装置に対応する画像形成装置の公開鍵を前記計

算装置で受信する第1の受信工程と、

ハッシングアルゴリズムを前記画像形成装置の公開鍵に適用して第1の画像形成装置の鍵ハッシュを作成するハッシング工程と、

前記画像形成装置で印刷されたテストページから取得し、前記計算装置に接続したユーザ入力手段で前記計算装置に入力する所定の第2の画像形成装置の鍵ハッシュを前記計算装置で受信する第2の受信工程と、

前記受信した画像形成装置の公開鍵の信頼性を検証するために、検証アルゴリズムを適用して前記第1の画像形成装置の鍵ハッシュと前記第2の画像形成装置の鍵ハッシュとを比較する検証工程と、

前記受信した画像形成装置の公開鍵の信頼性が前記検証工程で検証された場合、前記受信した画像形成装置の公開鍵を前記計算装置の記憶領域に格納する格納工程と、を有することを特徴とする情報処理方法。

【請求項23】 データの暗号化のための公開鍵を認証する装置において、

請求項1から22のいずれか1項に記載の情報処理方法を行うために実行可能な処理工程を格納するプログラムメモリと、

前記プログラムメモリに格納された処理工程を実行するプロセッサと、を有することを特徴とする装置。

【請求項24】 データの暗号化のための公開鍵を認証するためのコンピュータ可読媒体に格納されたコンピュータにより実行可能な情報処理方法であって、

請求項1から22のいずれか1項に記載の情報処理方法を行うために実行可能である処理工程を含むことを特徴とする情報処理方法。

【請求項25】 データの暗号化のための公開鍵を認証するためのコンピュータ実行可能な処理工程を格納するコンピュータ可読媒体において、

前記コンピュータ実行可能な処理工程は請求項1から22のいずれか1項に記載の情報処理方法を実施可能である処理工程を有することを特徴とする可読媒体。

【請求項26】 データの暗号化のための公開鍵を機密に格納し、情報装置に機密に格納されたユーザ固有の鍵対を利用し且つ、暗号化データを対象となる装置に送信する情報処理装置であって、

対象となる装置に対応する対象公開鍵を受信する受信手段と、

機密レジストリからユーザ固有の鍵対を取得する取得手段と、

前記ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して前記対象公開鍵に基づいて対象鍵を検証するためのプログラム又はデータを作成する鍵暗号化手段と、

前記対象鍵を検証するためのプログラム又はデータと前記対象公開鍵とを格納する格納手段と、

前記対象鍵を検証するためのプログラム又はデータと前記対象公開鍵とを前記格納手段から抽出する抽出手段

と、
前記対象公開鍵の信頼性を検証するために、前記ユーザ固有の鍵対からのユーザ固有の公開鍵を前記対象鍵を検証するためのプログラム又はデータに適用する検証手段と、
前記対象公開鍵の信頼性が検証された場合、データを前記対象公開鍵で暗号化することによって前記対象となる装置に送信するための暗号化データを作成するデータ暗号化手段と、を有することを特徴とする情報処理装置。
【請求項27】 暗号化プリントデータを画像形成装置に転送する情報処理装置であって、
前記画像形成装置から公開鍵を抽出する抽出手段と、
前記公開鍵から検証情報を生成する生成手段と、
印刷命令を認識する認識手段と、
前記印刷命令の認識に応答して、前記公開鍵が前記抽出した公開鍵から変更していないことを検証する検証手段と、
前記抽出した公開鍵が変更していないと検証された場合に、前記公開鍵を使用して暗号化処理を行い、前記抽出した公開鍵が変更したと検証された場合に暗号化処理を行わないように暗号化処理を制御する制御手段と、を有することを特徴とする情報処理装置。
【請求項28】 コンピュータに格納したユーザ固有の鍵を取得する取得手段と、
認証情報を入力する入力手段と、
前記取得手段が前記ユーザ固有の鍵を取得可能かどうかを判定する判定手段とを更に具備することを特徴とする請求項27に記載の情報処理装置。
【請求項29】 前記制御手段は暗号化処理を制御し、
取得手段で取得したユーザ固有の鍵を使用してプリントデータを暗号化し、前記公開鍵を使用して前記ユーザ固有の鍵を暗号化することを特徴とする請求項27に記載の情報処理装置。
【請求項30】 暗号化プリントデータを画像形成装置に転送する情報処理方法であって、
前記画像形成装置から公開鍵を抽出する抽出工程と、
前記公開鍵から検証情報を生成する生成工程と、
印刷命令を認識する認識工程と、
前記印刷命令の認識に応じて、前記公開鍵が前記抽出した公開鍵から変更していないことを検証する検証工程と、
前記抽出した公開鍵が変更していないと検証された場合に前記公開鍵を使用して暗号化処理を行い、前記抽出した公開鍵が変更したと検証された場合に暗号化処理を行わないように暗号化処理を制御する制御工程と、を有することを特徴とする情報処理方法。
【請求項31】 コンピュータに格納したユーザ固有の鍵を取得する取得工程と、
認証情報を入力する入力工程と、
前記取得工程で前記ユーザ固有の鍵を取得可能かどうか

を判定する判定工程とを更に含むことを特徴とする請求項30に記載の情報処理方法。

【請求項32】 前記制御工程は暗号化処理を制御し、
取得工程で取得したユーザ固有の鍵を使用してプリントデータを暗号化し、前記公開鍵を使用して前記ユーザ固有の鍵を暗号化することを特徴とする請求項30又は31に記載の情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置、方法、制御プログラムにおける暗号化処理に関するものである。

【0002】[文献の援用]1999年10月4日出願の米国特許出願第09/411,070号、名称「Targeted Secure Printing」を文献として援用する。

【0003】

【従来の技術】計算環境では、ネットワーク上の1箇所にあるコンピュータで生成された印刷ジョブを、他の場所にある画像出力装置で印刷することができる。例えば、パーソナルコンピュータ(PC)を離れた場所にあるプリンタに接続しても良いし、ワークステーションを多数の装置やワークステーションが存在するネットワークに接続しても良い。印刷ジョブが機密情報や他の取り扱いに注意を要する情報を含んでいる場合、印刷ジョブの発信元と送信先のプリンタとの間で印刷ジョブが無許可で傍受されてしまう可能性がある。特に、発信元のPCと送信先のプリンタとの間のローカル接続に接続されている無許可の装置や、発信元のワークステーションと送信先のプリンタとが存在するネットワークに接続されている装置によって印刷ジョブが傍受されてしまう可能性がある。このような無許可の装置は、ネットワーク盗聴ツール、ネットワークトラッキングツール、及びネットワーク傍受ツールを利用可能なPCやワークステーションであるかもしれない。

【0004】印刷ジョブの望ましくない傍受や抽出を回避するために、プリンタ公開鍵を利用して発信元のコンピュータでプリントデータを暗号化する機密印刷を使用することが知られている。プリンタ公開鍵を対称鍵と共に使用してプリントデータを暗号化するアプリケーションもある。暗号化プリントデータは送信先のプリンタに送られて、そこでプリンタ公開鍵を使用してプリントデータを復号化し格納する。プリンタ公開鍵はプリンタで機密に保持されて、暗号化プリントデータの機密保護を確実なものにする。コンピュータが画像形成装置の好適な一例であるプリンタ公開鍵を取得して格納することが好ましいが、プリンタ公開鍵が改変又は改竄されていないことを確認するために、プリンタ公開鍵を使用してプリントデータを暗号化する度にプリンタ公開鍵を検証するべきである。

【0005】暗号化処理用の公開鍵の機密配布及び検証

を容易にするために認証局を使用することが多い。認証局とは、ユーザへの機密配信のためにプリンタ製造業者などの開発者や製造業者に対して固有の公開鍵を署名できる第三者機関である。例えば、認証局は、プリンタ公開鍵の配信元と認証局とに関する情報と共に配信用の証明書にプリンタ公開鍵を添付して、証明書全体に署名することによって、認証局自身の秘密鍵を使用してプリンタ製造業者からのプリンタ公開鍵に署名できる。その後、ユーザは、使用する署名後のプリンタ公開鍵を含む証明書にアクセスできる。このような場合、ユーザは認証局自身の信用公開鍵（検証鍵）を取得して、この公開鍵を使用して署名されたプリンタ公開鍵が正規のものであることを検証する。それによって、対応するプリンタ秘密鍵を含む送信先のプリンタで印刷するユーザのプリントデータの暗号化に対して、ユーザがプリンタ公開鍵を信用することが可能となる。

【0006】プリンタ公開鍵などの装置の公開鍵の使用を望むユーザが認証局からの証明書を利用して公開鍵の信頼性を検証することは実用的でないことが多い。例えば、認証局は、証明書の保全性を維持するために時々その検証鍵を変更することが知られている。更に、証明書が期限切れになるか、又は認証局によって無効になる可能性もある。証明書の保全性を確実なものにするには、証明書の保全性を信頼する前に認証廃棄リスト（CRL）をチェックしなければならない。残念ながら、暗号化処理に対して特定の公開鍵を使おうとしている際に、毎回、ユーザが認証局の検証鍵を取得することは時間がかかってしまう。

【0007】加えて、全ての装置がその公開鍵の配信に認証局を使用するとは限らない。また、ユーザは、ユーザのアプリケーション毎に必要な異なる公開鍵をサポートするための対応する認証局からの多数の検証鍵を格納して保持しなければならない可能性もある。最後に、認証局からの証明書は署名された公開鍵に加えて付加情報を含んでいることが多く、この付加情報を処理することで、署名された公開鍵の検証時の処理のオーバーヘッドが増加してしまう。

【0008】

【発明が解決しようとする課題】そのため、証明書や認証局を必要とすることなく使用前に毎回、公開鍵を容易に検証できる計算装置において公開鍵を機密に保持できる構成が必要となる。

【0009】本発明は、プリンタなどの対象となる装置から公開鍵を取得して格納することによって、上記の問題を解決する。ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して、公開鍵に対応する対象鍵を検証するためのデータ又はプログラムを作成する。これに関して、対象鍵を検証するためのデータ又はプログラムとしては、本発明の目的に応じた複数の種類のデータオブジェクトのいずれか1つが可能である。例えば、対象鍵を検

証するためのデータ又はプログラムは、暗号化公開鍵、公開鍵のデジタル署名、又はDSSなどの機密保護アルゴリズムを公開鍵に適用して得られる他のデータオブジェクトから構成することが可能である。公開鍵が暗号化のために引き続き必要となる場合は、ユーザ固有の鍵対からのユーザ固有の公開鍵を使用して対象鍵を検証するためのデータ又はプログラムを復号化し、格納済みの公開鍵と比較することで、格納済みの公開鍵が変更又は改変されていないことを検証する。

【0010】

【課題を解決するための手段】そのため、本発明の一形態は、計算装置に機密に格納したユーザ固有の鍵対を使用して、計算装置のデータの暗号化のための公開鍵を機密に格納することに関する。特に、対象となる装置に対応する対象公開鍵を受信し、機密レジストリからユーザ固有の鍵対を取得し、ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して前記対象公開鍵に基づいて対象鍵を検証するためのデータ又はプログラムを作成する。対象鍵を検証するためのデータ又はプログラムと対象公開鍵とを記憶領域に格納する。続いて、対象鍵を検証するためのデータ又はプログラムと対象公開鍵とを記憶領域から抽出する。対象公開鍵の信頼性を検証するために、ユーザ固有の鍵対からのユーザ固有の公開鍵を対象鍵を検証するためのデータ又はプログラムに適用し、対象公開鍵の信頼性が検証された場合、データを対象公開鍵で暗号化することによって対象となる装置に送信するための暗号化データを作成する。

【0011】計算装置で実行するオペレーティングシステムが、ユーザ固有の鍵対を生成し機密に保持するのが好ましい。例えば、オペレーティングシステムは、各ユーザのユーザ固有の鍵対を格納し、ユーザ固有の鍵対に対応するユーザの適切なログイン識別が提供された時のみユーザ固有の鍵対へのアクセスを許可する機密レジストリを保持するのが好ましい。また、対象鍵を検証するためのデータ又はプログラムは、対象公開鍵をハッシングし、ユーザ固有の鍵対からのユーザ固有の秘密鍵で第1の鍵ハッシュを暗号化することによって作成された公開鍵署名であるのが好ましい。検証工程は、ユーザ固有の鍵対からのユーザ固有の公開鍵で対象鍵を検証するためのデータ又はプログラムを復号化して第1の鍵ハッシュを抽出することを含むのが好ましい。格納済みの対象公開鍵をハッシングして第2の鍵ハッシュを取得し、第1及び第2の鍵ハッシュを比較して、格納済みの対象公開鍵の信頼性を検証する。また、受信工程において、計算装置から対象となる装置への要求に応じて対象公開鍵を受信するのが好ましい。

【0012】上述の構成によって、データの暗号化で引き続き使用するために計算装置で対象公開鍵を機密に保持することができる。特に、対象公開鍵の暗号化（署名）とそれ以降の検証を局所的に保持されたユーザ固有

の鍵対で行うことによって、外部のデジタル証明書や認証局を必要とすることなく、使用する前に毎回、対象公開鍵を検証することが容易になる。

【0013】他の態様では、本発明は、計算装置に機密に格納したユーザ固有の鍵対を使用して、画像形成データの暗号化のための画像形成装置の公開鍵を計算装置に機密に格納することに関する。特に、画像形成装置に対応する画像形成装置の公開鍵を受信し、対応するユーザ識別に応じて機密レジストリからユーザ固有の鍵対を取得する。ハッシングアルゴリズムを画像形成装置の公開鍵に適用して第1の画像形成装置鍵ハッシュを作成し、暗号化アルゴリズムを適用してユーザ固有の鍵対からのユーザ固有の秘密鍵で第1の画像形成装置鍵ハッシュを暗号化することによって画像形成装置の鍵署名を作成する。この画像形成装置の鍵署名と画像形成装置の公開鍵とを記憶領域に格納する。続いて、画像形成装置の鍵署名と画像形成装置の公開鍵とを記憶領域から抽出する。ハッシングアルゴリズムを抽出した画像形成装置の公開鍵に適用して第2の画像形成装置の鍵ハッシュを作成し、復号化アルゴリズムを適用してユーザ固有の鍵対からのユーザ固有の公開鍵で画像形成装置の鍵署名を復号化することによって第1の画像形成装置の鍵ハッシュを抽出する。抽出した画像形成装置の公開鍵の信頼性を検証するために、検証アルゴリズムを適用して前記第1の画像形成装置の鍵ハッシュと第2の画像形成装置の鍵ハッシュとを比較し、抽出した画像形成装置の公開鍵の信頼性が検証された場合、抽出した画像形成装置の公開鍵を使用して暗号化アルゴリズムを画像形成データに適用することによって画像形成装置に送信するための暗号化プリントデータを作成する。

【0014】計算装置で実行するオペレーティングシステムが、取得工程で取得したユーザ固有の鍵対を生成し機密に保持するのが好ましい。例えば、オペレーティングシステムは、各ユーザのユーザ固有の鍵対を格納し、ユーザ固有の鍵対に対応するユーザの適切なログイン識別が提供された時のみユーザ固有の鍵対へのアクセスを許可する機密レジストリを保持するのが好ましい。また、受信工程において、計算装置から画像形成装置へ送られる鍵要求に応じて画像形成装置の公開鍵を受信するのが好ましい。

【0015】上述の構成によって、データの暗号化で引き続き使用するために計算装置で画像形成装置の公開鍵を機密に保持することができる。特に、画像形成装置の公開鍵の署名とそれ以降の検証を局所的に保持されたユーザ固有の鍵対で行うことによって、外部のデジタル証明書や認証局を必要とすることなく、使用する前に毎回、画像形成装置の公開鍵を検証することが容易になる。

【0016】本発明の更に他の態様によると、計算装置が受信した画像形成装置の公開鍵を認証する。特に、計

算装置は画像形成装置に対応する画像形成装置の公開鍵を受信し、ハッシングアルゴリズムを画像形成装置の公開鍵に適用して第1の画像形成装置の鍵ハッシュを作成する。計算装置は、画像形成装置で印刷されたテストページから取得した所定の第2の画像形成装置の鍵ハッシュを受信する。この第2の画像形成装置の鍵ハッシュは、計算装置に接続したユーザ入力手段で計算装置に入力される。受信した画像形成装置の公開鍵の信頼性を検証するために、検証アルゴリズムを適用して第1の画像形成装置の鍵ハッシュと第2の画像形成装置の鍵ハッシュとを比較し、受信した画像形成装置の公開鍵の信頼性が検証された場合、受信した画像形成装置の公開鍵を計算装置の記憶領域に格納する。

【0017】受信した画像形成装置の公開鍵は、計算装置から画像形成装置に送られた鍵要求メッセージに応じて受信するのが好ましい。加えて、テストページは計算装置のユーザからのコマンドに応じて印刷するのが好ましく、このコマンドは画像形成装置の前面パネルを介してユーザによって直接入力される。ユーザ入力手段はキーボードかマウスであるのが好ましく、これによってユーザはテストページから所定の第2のプリンタ鍵ハッシュを見ることができ、所定の第2の画像形成装置の鍵ハッシュを計算装置に入力することができる。

【0018】上述の構成によって、画像形成装置の公開鍵を画像形成装置から画像形成装置のユーザで最初に受信された後に認証することができる。特に、ユーザが存在する場合、受信した画像形成装置の公開鍵の認証を、画像形成装置で印刷された所定のハッシュ値を使用して行う。このように、外部のデジタル証明書や認証局を必要とすることなく、画像形成装置の公開鍵の信頼性を受信後に容易に検証する。

【0019】本発明の性質を即座に理解できるように、本発明の簡単な概要を提示した。添付の図面と関連させて以下の好ましい実施例の詳細な説明を参照することにより、本発明をより完全に理解することができるであろう。

【0020】

【発明の実施の形態】本実施形態は、他のデータ処理装置にも適用可能であるが、外部の認証局を必要とすることなく、検証済みのプリンタ鍵を使用してプリントデータを暗号化する機密印刷を行う環境を提供する。特に、本実施形態は、ユーザ固有の秘密鍵を使用して格納済みのプリンタ公開鍵の暗号化鍵バージョンを作成する。プリンタ公開鍵がプリントデータの暗号化のために引き続き必要となる場合は、暗号化鍵バージョンをユーザ固有の公開鍵を使用して復号化した後、格納済みのプリンタ公開鍵と比較して、格納済みのプリンタ公開鍵が変更又は改変されていないことを検証することになる。図1は、本発明の実施の形態を実現する計算環境のシステム図である。図1に示すように、計算環境は、コンピュー

タ10と、プリンタ20と、接続1とを備える。接続1としては、シリアル接続、USB接続、ファイアワイヤ接続又は他の接続などのコンピュータ10とプリンタ20との間の単純なローカル接続が可能である。代わりに、接続1は、バス型物理構造から成るイーサネットネットワーク媒体などのネットワークでも良い。接続1をインターネットを含む他の種類のネットワークで構成しても良いことは理解されるであろう。

【0021】デスクトップコンピュータ10は、Microsoft Windows（登録商標）2000、Microsoft Windows ME又はMicrosoft Windows XPなどのウィンドウイングオペレーティングシステム環境を有するパーソナルコンピュータやワークステーションであるのが好ましい。PCコンピュータの典型的として、デスクトップコンピュータ10は、ディスプレイ11と、キーボード15と、マウス14と、ホストプロセッサ12と、固定ディスク13と、フロッピー（登録商標）ドライブ及び／又は他の種類の記憶媒体（不図示）を有することが好ましい。本実施の形態に係る固定ディスク13の内容とコンピュータ10の動作は以下に更に詳述する。

【0022】プリンタ20も接続1によってコンピュータ10に接続されており、受信したプリントデータに基づいて記録媒体に画像を印刷できるレーザプリンタ又はインクジェットプリンタが好ましい。プリンタ20は、好ましくは固定ディスクである固定記憶装置21を有するが、ROMやEEPROMなどの他の形式のコンピュータメモリでも良い。本実施の形態に係る固定記憶装置21の内容とプリンタ20の動作は以下に更に詳述する。

【0023】図2は、本実施の形態に係るネットワーク化計算環境のシステム図である。図2に示すように、計算環境は、コンピュータ10と、プリンタ20と、サーバ30と、接続1とを備える。図2のコンピュータ10とプリンタ20は、図1を参照して説明したものと同一である。しかし、図2の接続1は、バス型物理構造から成るイーサネット（登録商標）ネットワーク媒体などのネットワーク接続であるのが好ましい。

【0024】図2に示すように、サーバ30も接続1に接続されている。サーバ30は、Microsoft Windows（登録商標）2000、Microsoft Windows（登録商標）ME又はMicrosoft（登録商標）Windows XPなどのウィンドウイングオペレーティングシステム環境を有するPC互換型コンピュータを備えることが好ましい。サーバ30は、多数のファイル、アプリケーション、及びデータを格納する大型固定ディスクであるのが好ましい固定ディスク31を有する。従って、サーバ30をファイルサーバ、又はプリントサーバなどの他の種類のサーバとして、コンピュータ10などの接続1上の他の装置で利用することができる。また、サーバ30は、接続1上の他の装置がインターネットなどの他のネットワークにアク

セスするためのゲートウェイとして機能しても良い。本発明の一実施の形態では、以下に更に詳述するように、サーバ30を使用してコンピュータ10が使用する公開鍵を格納する。

【0025】図3は、コンピュータ10の固定ディスク13の内容及びプリンタ20の固定記憶装置21の内容を説明する図である。本発明はプリンタ以外の装置で実施することもできるが、ここではプリンタと共に使用する場合の本実施の形態を述べる。図3に示すように、プリンタ20の固定記憶装置21は、プリンタ公開鍵25とプリンタ秘密鍵23とを含むプリンタ鍵対22を含む。鍵25と23は、プリントデータの暗号化及び復号化にそれぞれ使用する暗号化鍵である。特に、プリンタ公開鍵25は、プリンタ20の製造業者が作成して保持するのが好ましいが、プリンタ20のシステム管理者や他のシステムユーザがプリンタ20にインストールすることもできる。代わりに、プリンタ20自身がプリンタ公開鍵25を生成することもできる。

【0026】プリンタ公開鍵25は、機密暗号化方式でプリンタ20に送るプリントデータの暗号化で使用するために一般の人々がアクセスできるようになっている。プリンタ秘密鍵23もプリンタ公開鍵25に対応する暗号化鍵であり、プリンタ公開鍵25の作成者によって作成される。しかし、プリンタ秘密鍵23はプリンタ20内で厳密な機密保護の下に保持されており、プリンタ公開鍵25のようにアクセスすること及び／又はプリンタ20から削除することはできない。このように、プリンタ鍵対22の鍵23と25の両方にプリンタ20のみがアクセスすることができるので、暗号化プリントデータがプリンタ20に向かう途中で傍受されても、プリンタ20に送られた暗号化プリントデータを無許可の第三者が復号化することはできないことをプリンタ20のユーザに信用させることができる。

【0027】図3に戻ると、コンピュータ10の固定ディスク13が、オペレーティングシステム40と、レジストリ41と、鍵データベース50と、プリンタドライバ60と、記憶領域62とを含んでいることが判る。前述のように、オペレーティングシステム40はウィンドウイングオペレーティングシステムであるのが好ましく、特に暗号化アプリケーションプログラミングインタフェース（CAPI）を含むMicrosoft Windows（登録商標）オペレーティングシステムであるのが好ましい。例えば、Microsoft CAPIは、効率的なトランスペアレント方式でユーザ固有の暗号化鍵対を生成し、保持し、アクセスするトランスペアレント方式を提供する。特に、CAPIはコンピュータ10のユーザ毎にユーザ固有の鍵対を生成し、特定の対応するユーザに対して各ユーザ固有の鍵対をレジストリエントリに格納する。CAPI（Crypto API）では、対応するユーザがユーザ固有のパスワードなどの適切なユーザログイン識別を提供するこ

とでコンピュータ10にログインしたのでない限り、ユーザ固有の鍵対へのアクセスを許可しない。許可されたユーザに対してユーザ固有の鍵対を検索するために、C APIは関数呼出しをサポートしている。また、C APIは、ユーザ固有の公開鍵で暗号化又は署名された公開鍵などのデータの信頼性を検証するための関数呼出しなど、他の暗号化関数呼出しもサポートする。

【0028】データの暗号化署名やそれ以降の暗号化署名の検証をサポートするPGPなどのアプリケーションも存在するが、このようなアプリケーションはMicrosoft Windows CAPIの機能性に対して著しい欠点を有しているように見える。特に、PGPなどの他の暗号化アプリケーションでは、暗号化署名の作成に使用する鍵対の記憶をアプリケーションのユーザが保持しなければならない。そのため、このようなアプリケーションでは厳密な機密保護の下で鍵対を保持するわけではないので、コンピュータの無許可のユーザが鍵対にアクセスして使用することで、許可されたユーザの暗号化データにアクセスできてしまう機密保護侵害を起こす可能性が高くなる。

【0029】CAPIをサポートするMicrosoft Windowsオペレーティングシステムを使用するのが好ましいが、他の種類のオペレーティングシステムを使用して本発明を実施できることは理解されるであろう。このような場合、CAPIで説明したように、ユーザにトランスペアレントな機密方式でユーザ固有の鍵対を生成し、保持し、アクセスする限り、上述のユーザ固有の鍵対の生成、保持、及びアクセスを他の種類のオペレーティングシステムの機能によって行うことができるし、アプリケーションによって行うこともできる。

【0030】図3に戻ると、鍵データベース50はオペレーティングシステム40の構成要素であり、コンピュータ10のユーザに対してユーザ固有の鍵対を機密に生成して保持するのに使用する。特に、鍵データベース50はコンピュータ10の各ユーザに対するユーザエントリを含んでおり、各ユーザエントリは「ユーザ1」51に対応するエントリ中のユーザ固有の鍵対51などの対応するユーザ固有の鍵対を含む。各ユーザ固有の鍵対は、データオブジェクトの暗号化/署名と暗号化/署名されたデータオブジェクトの信頼性の検証に対する秘密鍵と公開鍵とを含む。例えば、ユーザ固有の鍵対51はユーザ固有の公開鍵53とユーザ固有の秘密鍵54とを含んでおり、これらは共に「ユーザ1」51に固有のものであり、且つこれに対応している。

【0031】レジストリ41は、コンピュータ10の各ユーザに対応するデータを保持するためにオペレーティングシステム40が使用する記憶領域である。特に、レジストリ41は各ユーザに対するエントリを含んでおり、このエントリにはログイン識別データが格納されており、他のユーザ固有のデータも格納されている。例えば、レジストリ41のユーザ1(42)に対するエント

リはログインID45とデジタル署名44とを含む。ログインID45は、コンピュータ10にログインするためにユーザ1が使用し、機密保護のためにユーザ1だけが知っているパスワードであるのが好ましい。デジタル署名44はプリンタ公開鍵25などの対象となる鍵の信頼性を検証するためのプログラム及びデータを含む対象鍵ベリファイアである。デジタル署名44は、ユーザ1に対応するユーザ固有の鍵対51によって作成されてレジストリ41に保持されるデジタル署名であるのが好ましい。代わりに、デジタル署名44を対象鍵の暗号化バージョンで構成することもできるし、DSSなどの機密保護アルゴリズムを対象鍵に適用して得られたコードで構成することもできる。デジタル署名44は以下に更に詳述する。

【0032】同じく図3に示されるように、プリンタドライバ60を使用して、テキスト文書、映像、図形、又は他の種類の画像であるような画像の印刷を行うためにプリンタ20に送られるプリントデータを生成する。プリンタドライバ60は、最適な印刷品質を確保してプリンタ20の特徴と特性をサポートするためにプリンタ20に対応するのが好ましい。本発明の好適な実施の形態では、以下に更に詳述するように、プリンタドライバ60は本実施の形態の機能性を実現するためのソフトウェアコードを含む。

【0033】図3の記憶領域62は、プリンタドライバ60がアクセスするための固定ディスク13の通常の記憶領域であるが、必ずしも機密でなくても良い。記憶領域62は、プリンタ公開鍵25と、暗号化(署名)アルゴリズム65と、ハッシングアルゴリズム68と、復号化(検証)アルゴリズム76と、鍵検証アルゴリズム77と、ハッシュ検証アルゴリズム84と、その他のアプリケーション58と、その他のファイル59とを含む。以下に更に説明するように、プリンタ公開鍵25はプリントデータを暗号化する際に使用するためにプリンタ20から取得した。

【0034】暗号化(署名)アルゴリズム65は、プリントデータやプリンタ公開鍵25などのデータオブジェクトを暗号化又はデジタル署名するためにプリンタドライバ60が使用する。加えて、本実施の形態に係る暗号化(署名)アルゴリズム65は、他の種類の機密保護アルゴリズムで構成することができる。ハッシングアルゴリズム68は、以下に更に説明するように、プリンタ公開鍵25などのデータオブジェクトのデジタルハッシュを行うために使用する。復号化(検証)アルゴリズム76は、以下に更に説明するように、プリンタ公開鍵25などの暗号化データオブジェクトを復号化したり、署名されたデータオブジェクトのデジタル署名を検証するために使用する。加えて、本実施の形態に係る復号化(検証)アルゴリズム76は、他の種類の機密保護アルゴリズムで構成することができる。鍵検証アルゴリズム77

は、以下に更に十分に説明するように、復号化公開鍵と格納済みの公開鍵とを比較して、格納済みの公開鍵の信頼性を確認するために使用する。ハッシュ検証アルゴリズム84は、以下に更に十分に説明するように、復号化公開鍵のハッシュ値と格納済みの公開鍵に対して新たに生成されたハッシュ値とを比較して、格納済みの公開鍵の信頼性を確認するために使用する。最後に、その他のアプリケーション58とその他のファイル59は、その他のアプリケーションと機能をサポートするためにプリンタドライバ60及び/又はコンピュータ10が使用する。

【0035】図4Aは、本発明の一実施の形態に係るプリンタ公開鍵25を機密に格納する方法を示すブロック図である。まず、プリンタ公開鍵25は、コンピュータ10からの鍵要求に応じてプリンタ20から取得するのが好ましい。図2に示す代替環境では、プリンタ公開鍵25は、コンピュータ10からの鍵要求に応じてサーバ30から取得することができる。サーバ30は、プリンタ公開鍵25をプリンタ20から事前に取得している。図4Aに示すように、ユーザ固有の秘密鍵54をプリンタ公開鍵25と共に暗号化アルゴリズム65に提供して暗号化プリンタ公開鍵67を生成し、これをサブエントリ44中の「ユーザ1」エントリ42下にあるレジストリ41に格納する。前述のように、ユーザ固有の秘密鍵54には、ユーザ1のログインID45に基づいてオペレーティングシステム40を介してアクセスするのが好ましい。このように、今後も使用するためにプリンタ公開鍵25を暗号化された方式でレジストリ41に機密に格納し、プリンタ公開鍵25を使用してプリントデータを暗号化する前にプリンタ公開鍵25の格納済みのバージョンを認証する。

【0036】図4Bは、プリンタ公開鍵25を完全に暗号化する代わりにデジタル署名する本発明の他の実施の形態を示す。署名は完全な暗号化よりも処理のオーバーヘッドが少ないので、署名方法は完全暗号化方法より好ましい。図4Bに示すように、まず、コンピュータ10の計算環境に応じてプリンタ公開鍵25をプリンタ20から直接取得するか又はサーバ30から取得する。その後、プリンタ公開鍵25に固有のプリンタ公開鍵ハッシュ値69を生成するデジタルハッシングアルゴリズム68を、プリンタ公開鍵25に対して行う。ハッシングアルゴリズム68は、ハッシングアルゴリズムを適用するデータオブジェクトに対応するハッシュ値を作成する既存の種類のハッシングアルゴリズムであるのが好ましい。

【0037】ユーザ固有の秘密鍵54をプリンタ公開鍵ハッシュ値69と共に暗号化アルゴリズム65に提供し、基本的にプリンタ公開鍵ハッシュ値69の暗号化形式であるデジタル署名70を作成する。その後、デジタル署名70は、サブエントリ44中の「ユーザ1」エン

トリ42下にあるレジストリ41に格納される。前述のように、ユーザ固有の秘密鍵54には、ユーザ1のログインID45に基づいてオペレーティングシステム40を介してアクセスするのが好ましい。このように、デジタル署名70を今後も使用するためにレジストリ41に機密に格納し、プリンタドライバ60がプリンタ公開鍵25を使用してプリントデータを暗号化する前にプリンタ公開鍵25の格納済みのバージョンを認証する。

【0038】図5Aは、プリンタ公開鍵25の使用に先立ってプリンタ公開鍵25の信頼性を検証するために図4Aに示すように作成して格納した暗号化プリンタ公開鍵67の使用を示すブロック図である。図5Aにおいて、印刷コマンド72はコンピュータ10のユーザから受信するが、所望のプリントデータを機密にプリンタ20に送るという指示を含んでいるのが好ましい。図5Aに示すように、ユーザ固有の公開鍵53には、前述のようにオペレーティングシステム40を介してアクセスするのが好ましい。ユーザ固有の公開鍵53を暗号化プリンタ公開鍵67と共に復号化アルゴリズム76に提供して復号化プリンタ公開鍵75を取得する。プリンタ公開鍵25は記憶領域62から抽出されるが、コンピュータ10が図2に示すようなネットワーク化環境にあるならば、プリンタ公開鍵25をサーバ30の固定ディスク31から抽出することができる。その後、復号化プリンタ公開鍵75と、記憶領域62から抽出したプリンタ公開鍵25とを鍵検証アルゴリズム77に提供してプリンタ公開鍵25の信頼性を検証する。鍵検証アルゴリズム77が、復号化プリンタ公開鍵75はプリンタ公開鍵25と一致すると判定した場合、プリンタ公開鍵25は正規のものであり、場合に応じてプリンタ20又はサーバ30から最初に取得して以来、変更又は改変が行われていないことになる。もし不一致ならば、使用前にサーバ30から取得した場合にプリンタ公開鍵25が改変又は変更されたことになる。そのため、プリンタドライバ60がコンピュータ10のディスプレイ11に表示するためエラーメッセージを生成し、場合に応じてプリンタ20又はサーバ30からプリンタ公開鍵25の新たな認証済みのコピーを再度取得するようにユーザを促すのが好ましい。

【0039】図5Bは、プリンタ公開鍵25の使用に先立ってプリンタ公開鍵25の信頼性を検証するために図4Bに示すように作成して格納したデジタル署名70の使用を示すブロック図である。図5Bにおいて、印刷コマンド72はコンピュータ10のユーザから受信するが、所望のプリントデータを機密にプリンタ20に送るという指示を含んでいるのが好ましい。図5Bに示すように、ユーザ固有の公開鍵53には、前述のようにオペレーティングシステム40を介してアクセスするのが好ましい。ユーザ固有の公開鍵53をデジタル署名70と共に復号化アルゴリズム76に提供して復号化プリンタ

公開鍵ハッシュ値79を取得する。プリンタ公開鍵25は記憶領域62から抽出されるが、コンピュータ10が図2に示すようなネットワーク化環境にあるならば、プリンタ公開鍵25をサーバ30の固定ディスク31から抽出することができる。

【0040】その後、プリンタ公開鍵25に対してハッシングアルゴリズム68を再度行い、新たなプリンタ公開鍵ハッシュ値80を生成する。そして、復号化プリンタ公開鍵ハッシュ値79と新たなプリンタ公開鍵ハッシュ値80とをハッシュ検証アルゴリズム84に提供してプリンタ公開鍵25の信頼性を検証する。ハッシュ検証アルゴリズム84が、復号化プリンタ公開鍵ハッシュ値79は新たなプリンタ公開鍵ハッシュ値80と一致すると判定した場合、プリンタ公開鍵25は正規のものであり、場合に応じてプリンタ20又はサーバ30から最初に取得して以来、変更又は改変が行われていないことになる。もし不一致ならば、プリンタ公開鍵25は改変又は変更されていることになる。例えば、最初にコンピュータ10がサーバ30からプリンタ公開鍵25のバージョンを取得して以来、プリンタ公開鍵25の新しいバージョンが作成されてプリンタ20からサーバ30にアップロードされている可能性もある。そのため、プリンタドライバ60がコンピュータ10のディスプレイ11に表示するためにエラーメッセージを生成し、場合に応じてプリンタ20又はサーバ30からプリンタ公開鍵25の新たな認証済みのコピーを再度取得するようにユーザを促すのが好ましい。

【0041】図6は、プリンタ公開鍵25が正規のものであると判定された場合のプリントデータの暗号化を説明するための図である。図6に示すように、ランダム鍵生成器82を使用して対称鍵83を生成する。対称鍵83はデータオブジェクトを暗号化及び復号化するのに使用できる暗号化鍵である。ランダム鍵生成器82はオペレーティングシステム40の関数であるのが好ましく、関数呼出しによってアクセスされる。プリントデータ85と対称鍵83とを暗号化アルゴリズム65に提供して暗号化プリントデータ87を生成する。この点に関して、プリンタ20は、印刷用に暗号化プリントデータ87を復号化するために対称鍵83の機密コピーが必要となる。このため、プリンタ公開鍵25と対称鍵83とを暗号化アルゴリズム65に提供して暗号化対称鍵88を生成する。このように、対称鍵を機密にプリンタ20に渡すことができる。その後、暗号化対称鍵88をプリントジョブ89のヘッダ90に配置するが、プリントジョブ89は暗号化プリントデータ87も含んでいる。プリントジョブ89は接続1を介してプリンタ20に送られる。プリントジョブ89がプリンタ20に向かう途中で傍受されても、プリンタ20に機密に格納されたプリンタ秘密鍵23を使用せずに暗号化対称鍵88を復号化することはできないので、暗号化プリントデータ87を適

切に復号化することはできない。

【0042】図7はプリンタ20内の暗号化プリントデータ87の復号化を説明するための図である。図7に示すように、プリントジョブ89はプリンタ20で受信される。プリンタ秘密鍵23にはプリンタ20の固定記憶装置21からアクセスして、対称鍵83を抽出するためにプリントジョブヘッダ90からの暗号化対称鍵88と共に復号化アルゴリズム92に提供する。平文のプリントデータ85を生成するために、対称鍵83を暗号化プリントデータ87と共に復号化アルゴリズム92に提供する。その後、プリントデータ85をプリンタ20のプリントエンジン27に渡して、プリンタ20が記録媒体に印刷出力を生成して印刷画像100を作成する。このように、プリンタ公開鍵25の信頼性の検証に外部の認証局を使用することなく、プリンタ公開鍵25を使用してプリントデータを毎回、機密にプリンタ20に渡す。

【0043】図8は、本実施の形態に係る公開鍵、特にプリンタ公開鍵の使用を説明するためのフローチャートである。ステップS801において、ユーザは、好ましくはパスワードを使用して、コンピュータ10にログオンする。説明の便宜上、ユーザ1を例示するが、ユーザ1はログインID45を提供してコンピュータ10を使用する権限があることを検証する。次に、ステップS802において、ユーザ固有の鍵対51をユーザ1の識別に基づいて鍵データベース50から取得する。ステップS803において、プリンタ20から（コンピュータ10が図2に示すようなネットワーク化環境にあるならば、サーバ30から）コンピュータ10にプリンタ公開鍵25を送る。プリンタ公開鍵25は、場合に応じてプリンタ20又はサーバ30にコンピュータ10から送られた鍵要求に応じて送出するのが好ましい。ステップS804において、場合に応じてプリンタ20又はサーバ30からプリンタ公開鍵25を受信する。ステップS805において、図4Bを参照して説明したようにプリンタ公開鍵25に署名するのが好ましいが、代わりに、図4Aを参照して説明したようにプリンタ公開鍵25を暗号化しても良い。

【0044】ステップS805におけるこの2つの可能性を図9及び10にそれぞれ示す。図9に示すように、ユーザ固有の秘密鍵54を使用して暗号化アルゴリズム65に沿ってプリンタ公開鍵25を完全に暗号化することによって、暗号化プリンタ公開鍵67を作成する（S901）。その後、フローは図9の「戻る」（S902）に進む。図10に示すように、ハッシングアルゴリズム68をプリンタ公開鍵25に適用してプリンタ公開鍵ハッシュ値69を作成する（S1001）。ステップS1002において、プリンタ公開鍵ハッシュ値69をユーザ固有の秘密鍵54で暗号化してデジタル署名70を作成する。その後、フローは図10の「戻る」（S1003）に進む。

【0045】図8に戻ると、フローはステップS806に進み、プリンタ公開鍵25を今後も使用するために記憶領域62に格納し、デジタル署名70（または暗号化プリンタ公開鍵67）をレジストリ41に機密に格納する。代わりに、コンピュータ10が図2に示すようにサーバ30を有するネットワーク化環境にある場合は、プリンタ公開鍵25を記憶領域62に格納する代わりにサーバ30の固定ディスク31に格納できることは理解されるであろう。前述のように、コンピュータ10が図2に示すようにネットワーク化計算環境にある場合は、プリンタ公開鍵25をサーバ30の固定ディスク31に格納できる。このような場合、コンピュータ10がこれ以降にデータを暗号化する必要がある度に、コンピュータ10がサーバ30からプリンタ公開鍵25にアクセスするのが好ましい。これによって、サーバ30に格納されたプリンタ公開鍵25のバージョンがシステム管理者によって更新されたことをプリンタドライバが自動的に検出することが可能となる。ステップS807において、コンピュータ10はユーザ1から印刷コマンド72を受信するが、印刷コマンド72はプリントデータを機密にプリンタ20に送るという指示を含んでいるのが好ましい。

【0046】次に、プリンタ公開鍵25を、場合に応じて記憶領域62又はサーバ30の固定ディスク31から抽出する（ステップS808）。ステップS809において、デジタル署名70又は暗号化プリンタ公開鍵67を復号化し、プリンタ公開鍵25と共に検証アルゴリズムに提供してプリンタ公開鍵25の信頼性を検証する。図9及び10を参照して説明したように、プリンタ公開鍵25に署名するのか又は完全に暗号化するのかによってこのステップは異なる。図11はプリンタ公開鍵25を完全に暗号化する場合のステップS809の説明を示す。ステップS1101において、ユーザ固有の公開鍵53を使用して、レジストリ41から抽出した暗号化プリンタ公開鍵67を復号化する。次に、ステップS1102において、復号化プリンタ公開鍵75と抽出したプリンタ公開鍵25とを、それらが一致しているかどうかを検証するための鍵検証アルゴリズム77に提供することによって、プリンタ公開鍵25は正規のものであり、プリントデータを適切に暗号化するのに使用できると判定する。その後、フローはステップS1103の「戻る」に進む。

【0047】図12はプリンタ公開鍵25にデジタル署名してデジタル署名70を作成する場合を示す。ステップS1201において、ユーザ固有の公開鍵53を使用して、レジストリ41から抽出したデジタル署名70を復号化することによって、復号化プリンタ公開鍵ハッシュ値79を取得する。次に、ステップS1202において、新たなプリンタ公開鍵ハッシュ値80を取得するために、場合に応じて記憶領域62又はサーバ30から抽

出したプリンタ公開鍵25にハッシングアルゴリズム68を適用する。ステップS1203において、復号化プリンタ公開鍵ハッシュ値79と新たなプリンタ公開鍵ハッシュ値80とをハッシュ検証アルゴリズム84に提供してこれら2つのハッシュ値が一致するかどうかを判定し、これによってプリンタ公開鍵25の信頼性を確認する。その後、フローはステップS1204の「戻る」に進む。

【0048】図8に戻ると、フローはステップS810に進み、ステップS809で行われた検証で一致していたかを判定する。一致していたならば、フローはステップS812に進む。一致していないならば、フローはステップS811に進み、コンピュータ10のディスプレイ11に表示するためにエラーメッセージを生成した後、ステップS819の「戻る」に進む。ステップS812において、ランダム鍵生成器82を使用して対称鍵83を生成する。ステップS813において、暗号化アルゴリズム65を使用して対称鍵83でプリントデータ85を暗号化して暗号化プリントデータ87を生成する。次に、ステップS814において、暗号化アルゴリズム65を使用して検証済みのプリンタ公開鍵25で対称鍵83を暗号化して暗号化対称鍵88を生成する。暗号化対称鍵88と暗号化プリントデータ87とをプリントジョブ89に配置してプリンタ20に送る（ステップS815）。その後、フローはステップS816に進み、プリンタ20はプリントジョブ89を受信し、復号化アルゴリズム92を介してプリンタ秘密鍵23を適用して暗号化対称鍵88を復号化し、これによって対称鍵83を抽出する。対称鍵83を暗号化プリントデータ87に適用して復号化（明文の）プリントデータ85を抽出する（ステップS817）。復号化プリントデータ85はプリンタ20のプリントエンジン27に送られて、プリントデータ85に基づき印刷画像100を生成する（ステップS818）。その後、フローはステップS819の「戻る」に進む。

【0049】図13は、プリンタ20から受信したプリンタ公開鍵25などの受信公開鍵の初期認証のための本実施の形態に係る好適な構成を示す。特に、コンピュータ10がプリンタ公開鍵25の正しいコピーを受信したことを確認するために、プリンタ公開鍵25をコンピュータ10が最初に取得する場合に本構成によって認証を行う。図13に示すように、プリンタ公開鍵25をプリンタ20から取得してハッシングアルゴリズム68を行い、プリンタ公開鍵ハッシュ値69を生成する。

【0050】次に、好ましくは、コンピュータ10のユーザによってプリンタ20の前面で入力されたコマンドに応じて、プリンタテストページ102をプリンタ20で生成する。プリンタテストページは、プリンタ公開鍵25に対する正しいハッシュ値である印刷ハッシュ値103を含んでいる。印刷ハッシュ値103はユーザによ

ってコンピュータ10に入力されて、プリンタ公開鍵ハッシュ値69と共にハッシュ検証アルゴリズム84に提供される。このハッシュ検証アルゴリズム84は、受信したプリンタ公開鍵25の信頼性を検証するためにこれら2つのハッシュ値が一致するかどうかを判定する。一致するならば、コンピュータ10はプリンタ公開鍵25をプリンタ20からの正規のコピーとして受け付け、今後も使用するためにプリンタ公開鍵25を記憶領域62に格納する。一致しないならば、コンピュータ10のディスプレイ11に表示するためにエラーメッセージを生成し、プリンタ公開鍵25に対して他の要求をプリンタ20に送る又は印刷ハッシュ値103をコンピュータ10に再入力するなどの行動を起こすようにユーザを促す。

【0051】図14は、図13に示すプリンタ公開鍵25の初期認証を説明するためのフローチャートである。ステップS1401において、プリンタ公開鍵25をプリンタ20から要求する。ステップS1402において、プリンタ20はプリンタ公開鍵25をコンピュータ10に送る。プリンタ公開鍵25に対してハッシングアルゴリズム68を行い、プリンタ公開鍵ハッシュ値69を生成する(ステップS1403)。次に、好ましくは、コンピュータ10のユーザによってプリンタ20の前面で入力されたコマンドに応じて、プリンタテストページ102をプリンタ20で生成する。このプリンタテストページは、プリンタ公開鍵25に対する正しいハッシュ値である印刷ハッシュ値103を含んでいる。

【0052】ステップS1405において、好ましくは、コンピュータ10のディスプレイ11上に提供されたダイアログウィンドウから、印刷ハッシュ値103がユーザによってコンピュータ10に入力される。ステップS1406において、印刷ハッシュ値103はプリンタ公開鍵ハッシュ値69と共にハッシュ検証アルゴリズム84に提供される。ハッシュ検証アルゴリズム84は、受信したプリンタ公開鍵25の信頼性を検証するために、これら2つのハッシュ値が一致するかどうかを判定する。一致するならば、フローはステップS1409に進み、コンピュータ10はプリンタ公開鍵25をプリンタ20からの正規のコピーとして受け付け、今後も使用するためにプリンタ公開鍵25を記憶領域62に格納する。その後、フローはステップS1410に進む。ステップS1407において一致しないならば、フローはステップS1408に進み、コンピュータ10のディスプレイ11に表示するためにエラーメッセージを生成し、プリンタ公開鍵25に対して他の要求をプリンタ20に送る又は印刷ハッシュ値103をコンピュータ10に再入力するなどの行動を起こすようにユーザを促す。その後、フローはステップS1410の「戻る」に進む。

【0053】このように、暗号化するために公開鍵が必

要になる度に外部の認証局を使用して公開鍵の信頼性を検証する必要がなく、公開鍵の使用を通じて機密印刷を提供する。特に、プリンタの公開鍵などの対象公開鍵を今後も使用するためにコンピュータに機密に保持してデータを暗号化することができる。そのため、対象公開鍵の暗号化(署名)とそれ以降の検証を、局所的に保持されたユーザ固有の公開鍵で局所的に行うことによって、使用する前に毎回、対象公開鍵の信頼性を検証することが容易になる。

【0054】以上説明したように本実施形態の一つの側面によれば、暗号化するために公開鍵が必要になる度に外部の認証局に問い合わせる公開鍵の信頼性を検証する必要がなくなる。

【0055】また、本願実施形態の別の側面によれば、負荷の小さな処理で機密性の高い通信処理又はデータ処理環境を提供することができる。

【0056】

【発明の効果】以上説明したように本発明によれば、暗号化するために公開鍵が必要になる度に外部の認証局に問い合わせる公開鍵の信頼性を検証する必要がなくなるという効果がある。

【0057】本発明を特定の実施例によって説明した。本発明は上述の実施の形態には限定されず、当業者により本発明の趣旨から逸脱せずに様々な変更及び変形を実施しうることは理解されるであろう。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係る計算環境を表す図である。

【図2】本発明の他の実施の形態に係るネットワーク化計算環境を表す図である。

【図3】図1に示すコンピュータ及びプリンタの内部構造を示す詳細なブロック図である。

【図4A】本発明の一実施の形態に係る公開鍵の暗号化を説明するためのブロック図である。

【図4B】本発明の他の実施の形態に係る公開鍵の暗号化を説明するためのブロック図である。

【図5A】本発明の一実施の形態に係る格納済みの公開鍵の検証を説明するためのブロック図である。

【図5B】本発明の他の実施の形態に係る格納済みの公開鍵の検証を説明するためのブロック図である。

【図6】本実施の形態に係るプリントデータの暗号化を説明するためのブロック図である。

【図7】本実施の形態に係るプリントデータの復号化を説明するためのブロック図である。

【図8A】本発明の実施の形態に係る公開鍵の使用を説明するためのフローチャートである。

【図8B】本発明の実施の形態に係る公開鍵の使用を説明するためのフローチャートである。

【図9】本発明の一実施の形態に係る公開鍵の暗号化を説明するためのフローチャートである。

【図10】本発明の他の実施の形態に係る公開鍵の署名を説明するためのフローチャートである。

【図11】本発明の一実施の形態に係る格納済みの公開鍵の検証を説明するためのフローチャートである。

【図12】本発明の他の実施の形態に係る格納済みの公

開鍵の検証を説明するためのフローチャートである。

【図13】本発明の一実施の形態に係る受信公開鍵の初期検証を説明するためのブロック図である。

【図14】本発明の一実施の形態に係る受信公開鍵の初期検証を説明するためのフローチャートである。

【図1】

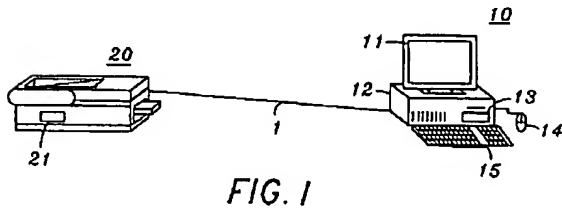


FIG. 1

【図2】

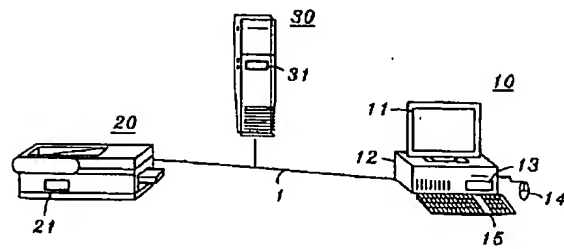


FIG. 2

【図3】

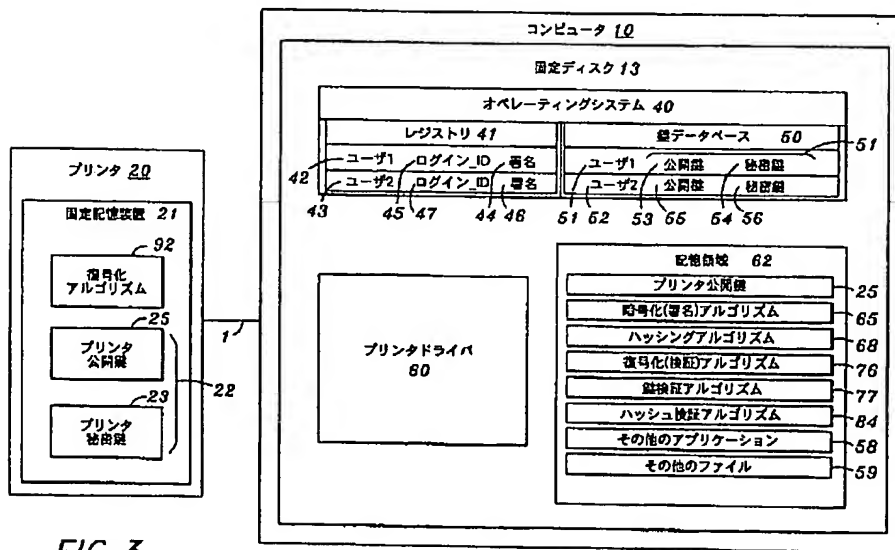


FIG. 3

【図4A】

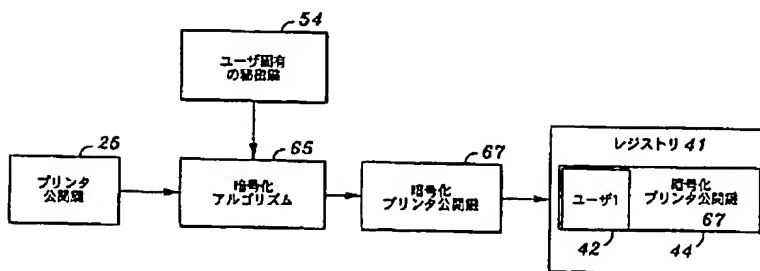


FIG. 4A

【図4B】

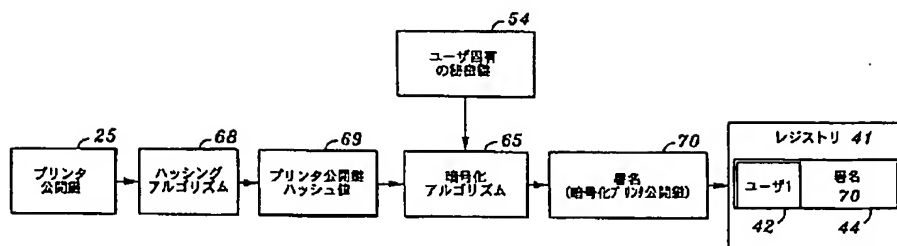


FIG. 4B

【図5A】

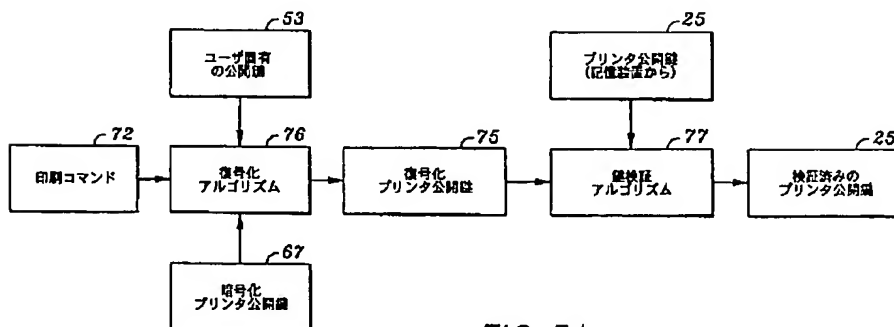


FIG. 5A

【図5B】

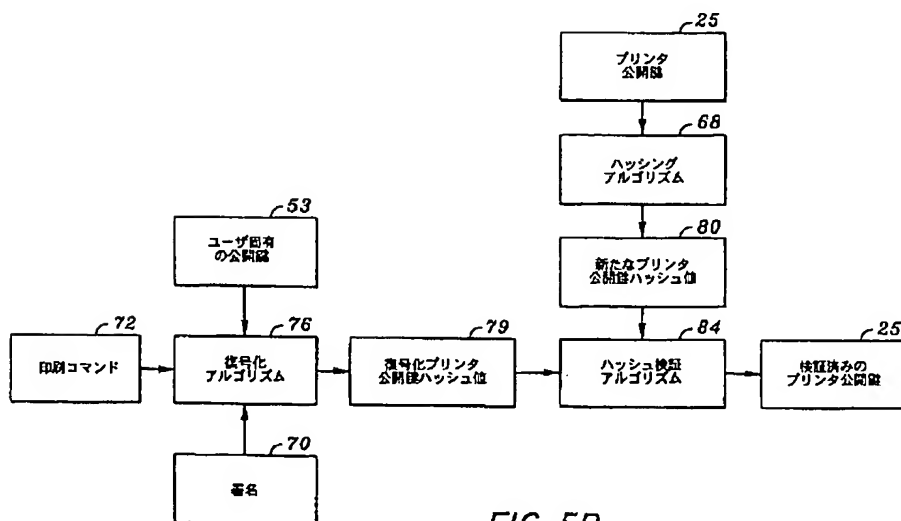


FIG. 5B

【図6】

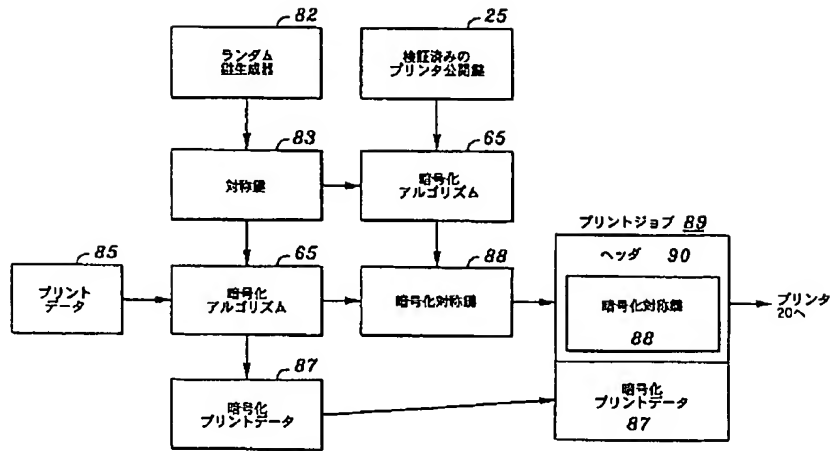


FIG. 6

【図7】

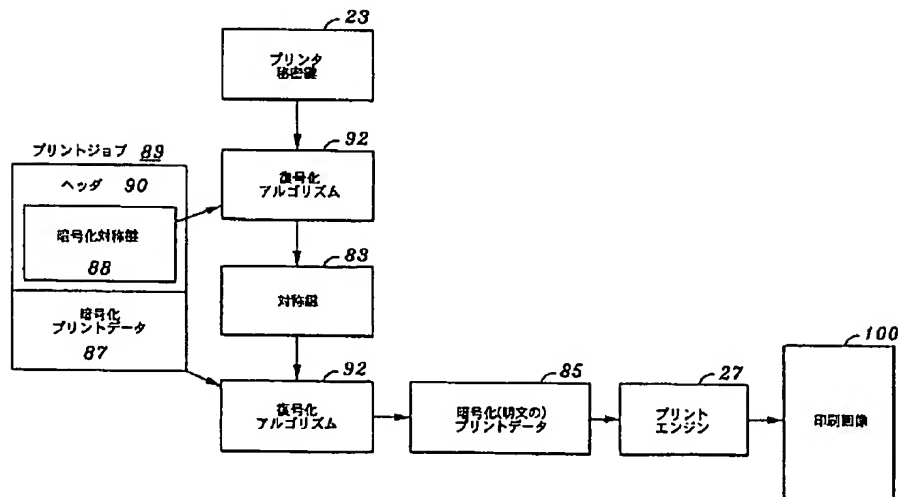
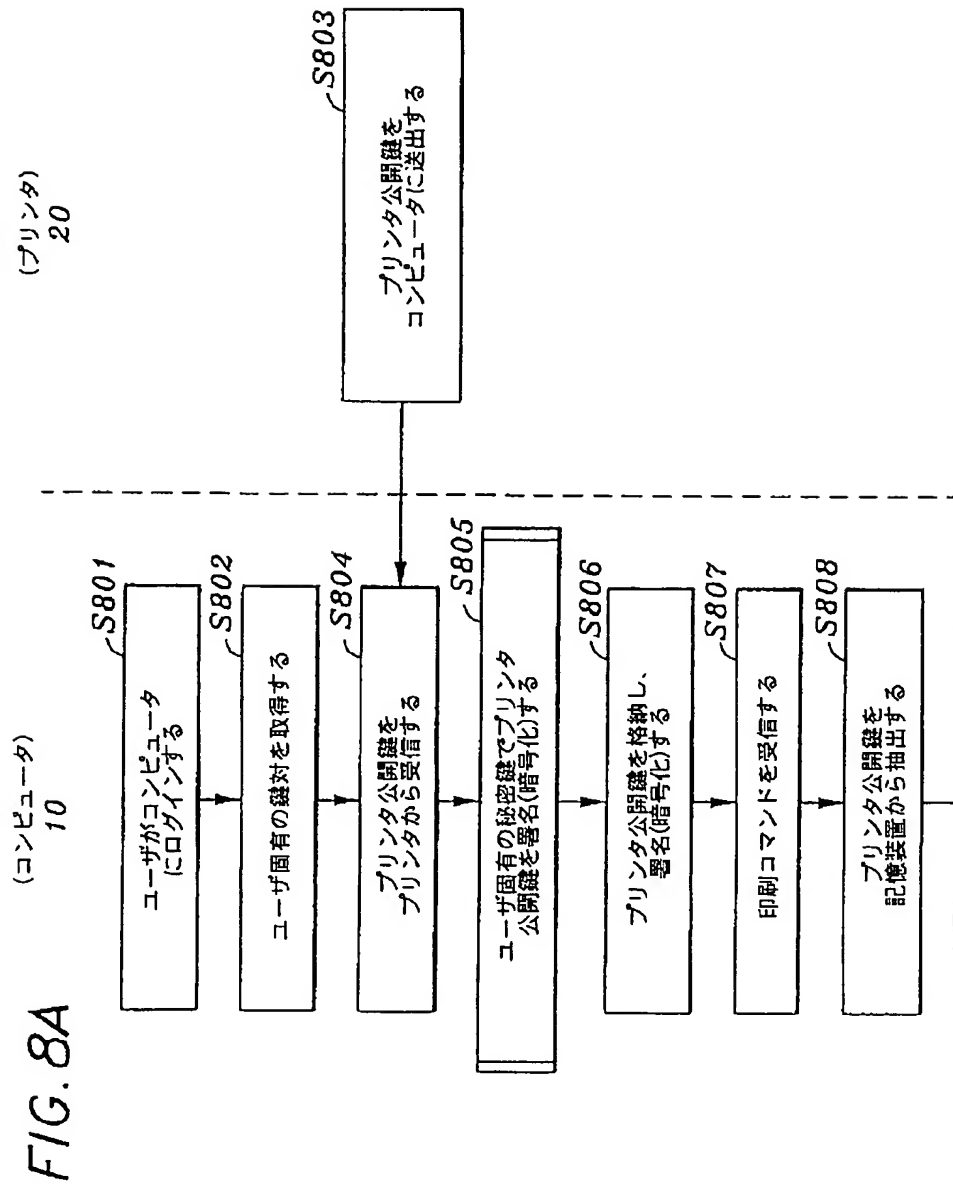
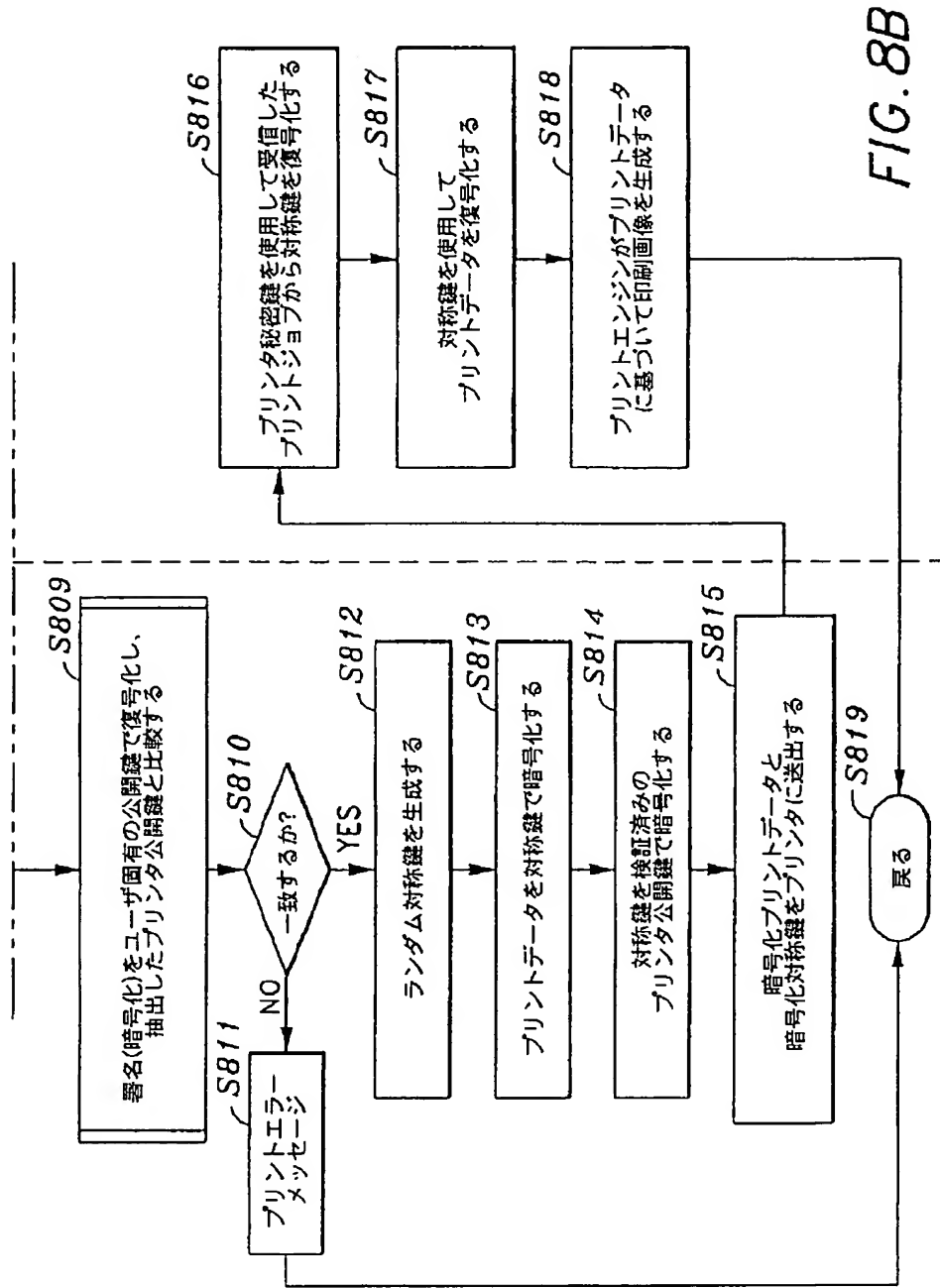


FIG. 7

【図8A】



【図8B】



【図9】

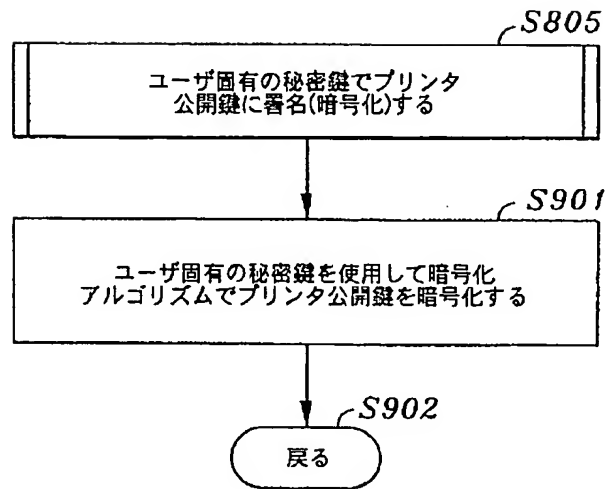


FIG. 9

【図10】

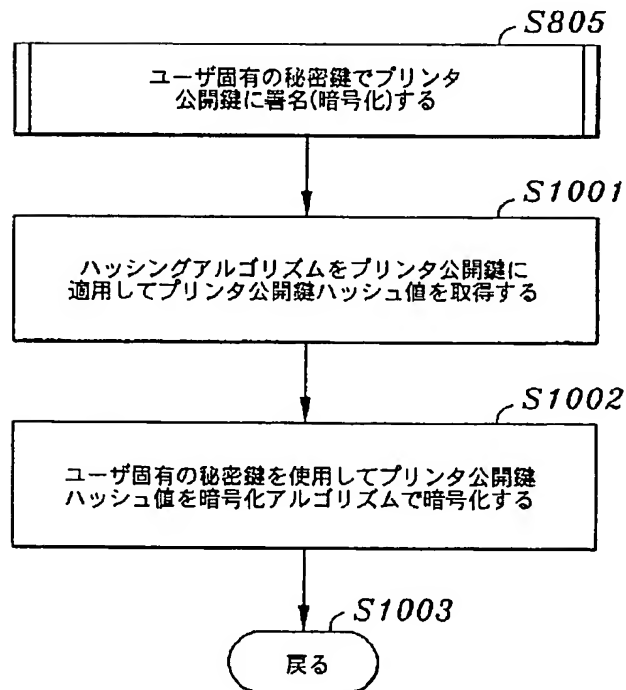


FIG. 10

【図11】

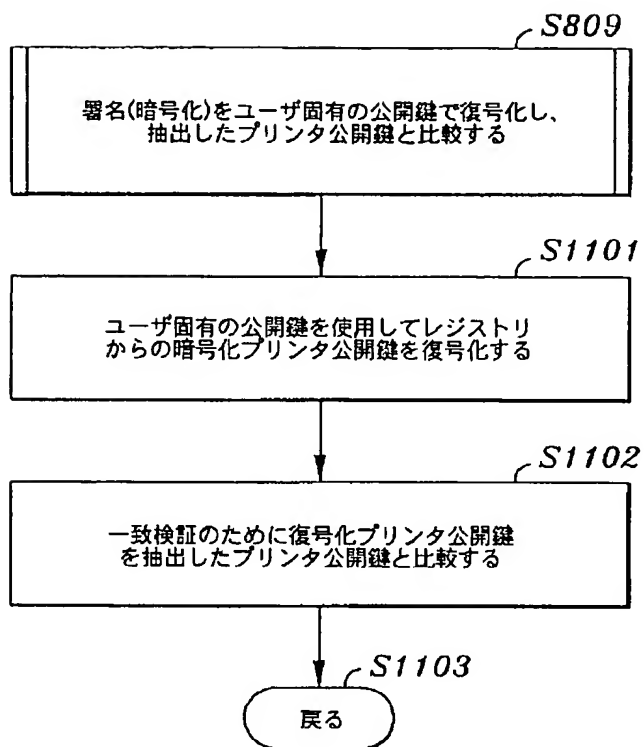


FIG. 11

【図13】

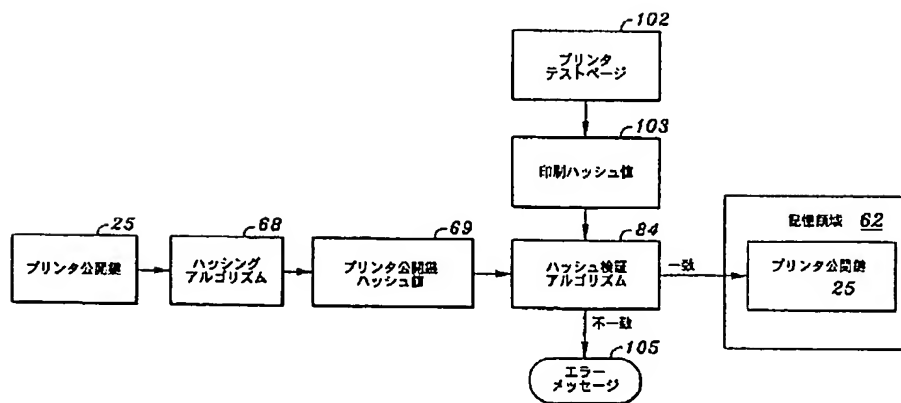


FIG. 13

【図12】

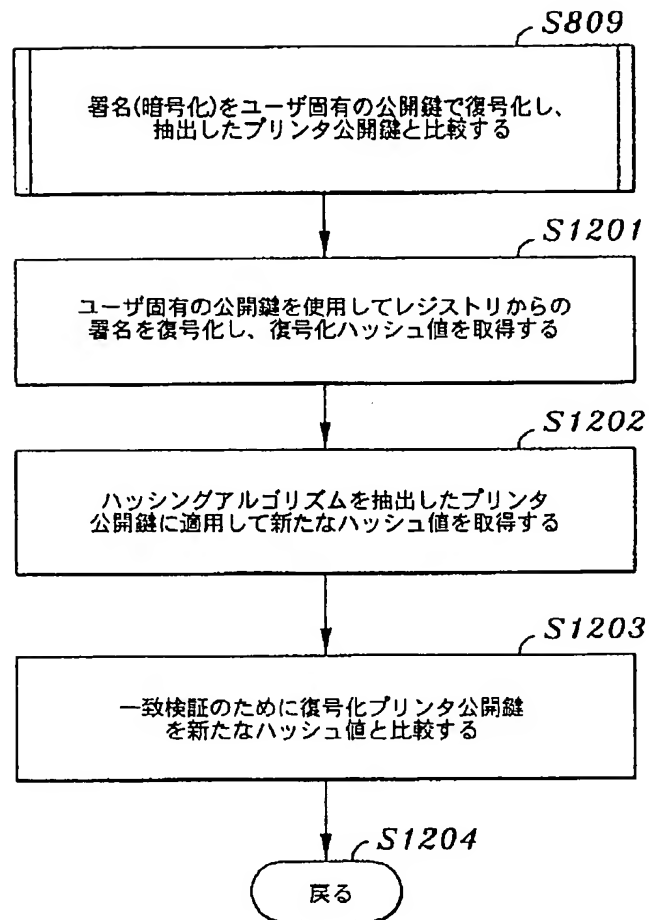


FIG. 12

【図14】

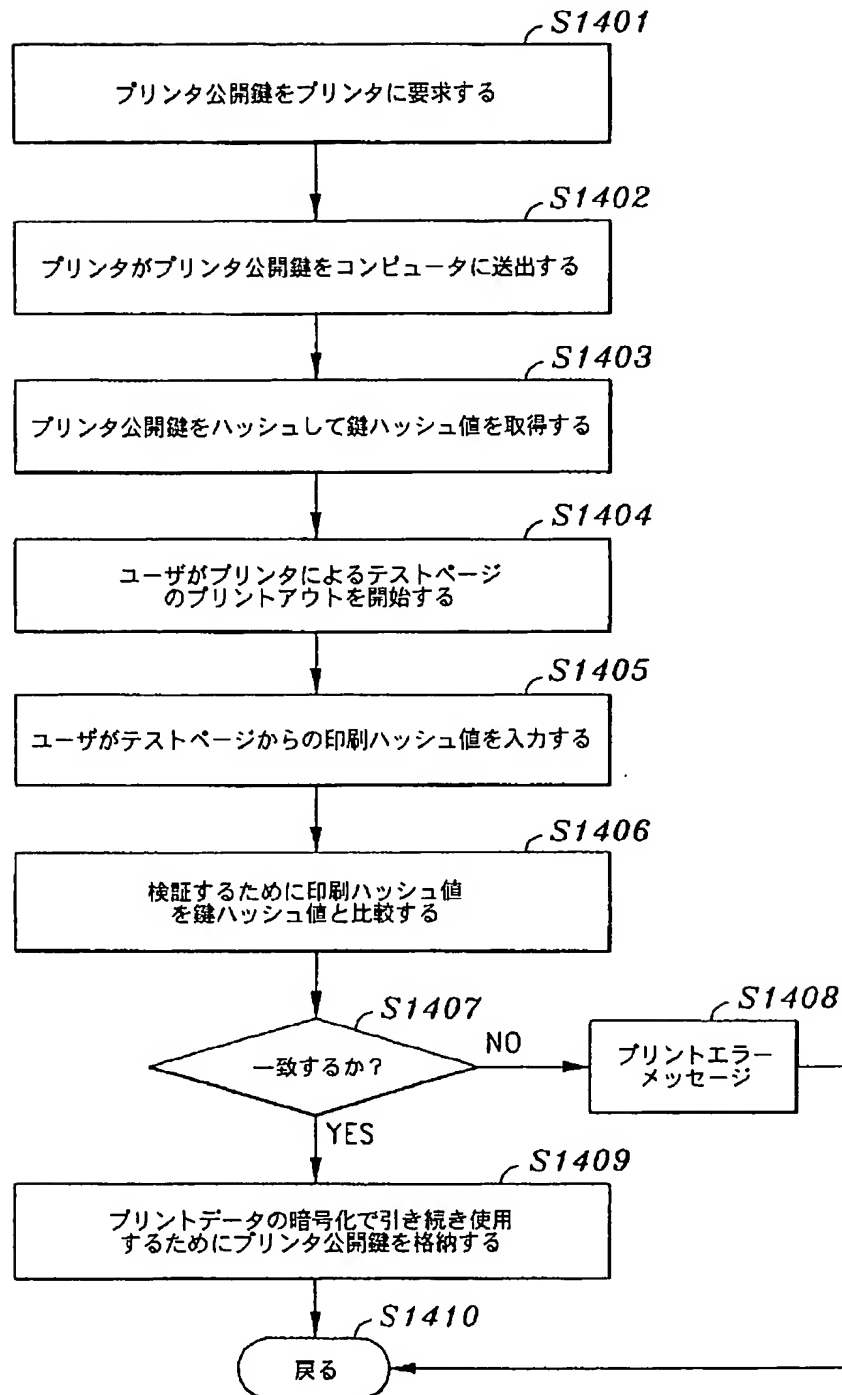


FIG. 14

フロントページの続き

(72)発明者 ウィリアム ツァン
アメリカ合衆国 カリフォルニア州
92612, アーバイン, イノベーション ド
ライブ 110 キヤノン デベロッパメン
ト アメリカス, インコーポレイテッド
内

(72)発明者 ドン フランシス パープラ
アメリカ合衆国 カリフォルニア州
92612, アーバイン, イノベーション ド
ライブ 110 キヤノン デベロッパメン
ト アメリカス, インコーポレイテッド
内

(72)発明者 ニール ワイ. イワモト
アメリカ合衆国 カリフォルニア州
92612, アーバイン, イノベーション ド
ライブ 110 キヤノン デベロッパメン
ト アメリカス, インコーポレイテッド
内

(72)発明者 クレイグ マザガット
アメリカ合衆国 カリフォルニア州
92612, アーバイン, イノベーション ド
ライブ 110 キヤノン デベロッパメン
ト アメリカス, インコーポレイテッド
内

Fターム(参考) 5B017 AA03 BB09 CA16
5B021 AA30 BB09 CC05
5J104 AA09 AA16 EA05 LA03 LA06